

Manuel Utilisateur Module Contrôle d'Accès

Pour utilisation avec ProSys 16, ProSys 40, et ProSys 128

Remarques importantes

Pour ce manuel les conditions et restrictions sont les suivantes:

- ✦ Ce manuel contient des informations qui sont la propriété de RISCO Group. De telles informations sont exclusivement distribuées pour aider de façon correcte et explicite les utilisateurs autorisés du système.
- ♦ Aucune partie du contenu de ce manuel ne peut être utilisée à d'autre fin, ni communiquée à d'autre personne ou société ni être reproduite de quelque façon que ce soit, ni électroniquement, ni mécaniquement, sans le consentement préalable formel et écrit de RISCO Group.
- ♦ Le texte et les représentations graphiques sont exclusivement destinés à l'illustration et comme explication. Les spécifications sur lesquelles ils sont basés sont soumises à des modifications sans communication préalable.
- ♦ Les informations de ce document pourront être soumises à des modifications sans aucune communication préalable. Noms de sociétés et de personnes et données utilisés comme exemple dans ce manuel sont fictifs, à moins que mentionné autrement.

Contenu

Chapitre 1: Introduction au module de contrôle d’accès

Le module contrôle d’accès, qui est intégré dans votre système de sécurité, est conçu pour une utilisation dans de petites et moyennes entreprises. Ce module est généralement utilisé là où un contrôle est nécessaire en vue de savoir quels utilisateurs ont eu accès à quelles portes / pièces d’un bâtiment. Sur le module contrôle d’accès, divers périphériques peuvent être raccordés tel que lecteurs de cartes, serrures électriques, détecteurs de mouvement, etc.

Un maximum de huit modules contrôle d’accès peuvent être raccordés sur la centrale ProSYS. De plus chaque module accepte deux lecteurs, ce qui fait que le système de protection est capable de contrôler un maximum de 16 portes.

Le module contrôle d’accès peut être programmé avec un clavier LCD installé ou au moyen du programme « Upload/Download ».

Définitions et prescriptions du contrôle d’accès

La liste ci-dessous donne les définitions et prescriptions en rapport avec le module contrôle d’accès:

- **Utilisateurs pour Activer/Désactiver:** Attribuer aux utilisateurs des droits d’accès qui leurs permettent d’activer et désactiver le système. Un maximum de 99 utilisateurs pour activer/désactiver peuvent être présents dans le système. Il est conseillé d’attribuer le même code PIN dans le module contrôle d’accès que celui qui est attribué à l’utilisateur dans le système de protection.
- **Utilisateurs Standards:** Attribuer aux utilisateurs des droits d’accès qui leurs permettent seulement d’ouvrir les portes; pas d’activation/désactivation du système. Un maximum de 999 utilisateurs pour entrée/sortie peuvent être présents dans le système.
- **Schéma horaire:** Définir des fenêtres de temps spécifiques qui déterminent quand les utilisateurs ont accès au système.
- **Groupe d’accès:** Un groupe d’utilisateurs qui a seulement accès au système via des portes spécifiques durant des périodes de temps déterminées. Un maximum de 16 groupes d’accès peuvent être configurés dans le système.
- **Code Carte:** Un code composé de 8 chiffres sur une carte d’accès qui est introduit dans le système afin d’attribuer des droits d’accès à un utilisateur.
- **Code PIN (Numéro d’Identification Personnel):** Aussi appelé code utilisateur. Un code de 4 chiffres qui est attribué à un utilisateur pour permettre à cet utilisateur de commander le système via un clavier installé. Le code PIN peut être utilisé à la place de la carte d’accès ou en plus de la carte d’accès.
- **RTE (Request to Exit):** Un bouton ou un détecteur de mouvement qui, lorsqu’il est activé, ouvre une porte spécifique en envoyant un signal au relais de porte.

- **Lecteur:** Le module contrôle d'accès accepte quatre types de lecteurs: Carte seul, Clavier seul, Carte ET Clavier et Carte OU Clavier.
- **Partition:** Un sous-système dans le système de sécurité qui peut être piloté comme un système séparé.
- **Mémoire Evénement** Chaque module contrôle d'accès peut stocker au maximum 1.000 événements dans la mémoire. Les événements peuvent être imprimés sur une imprimante locale ou être chargé à l'aide du programme « Upload/Download », conformément aux critères spécifiques.

Caractéristiques selon Centrale

Le tableau suivant contient les caractéristiques du système, selon le modèle de ProSYS installé.

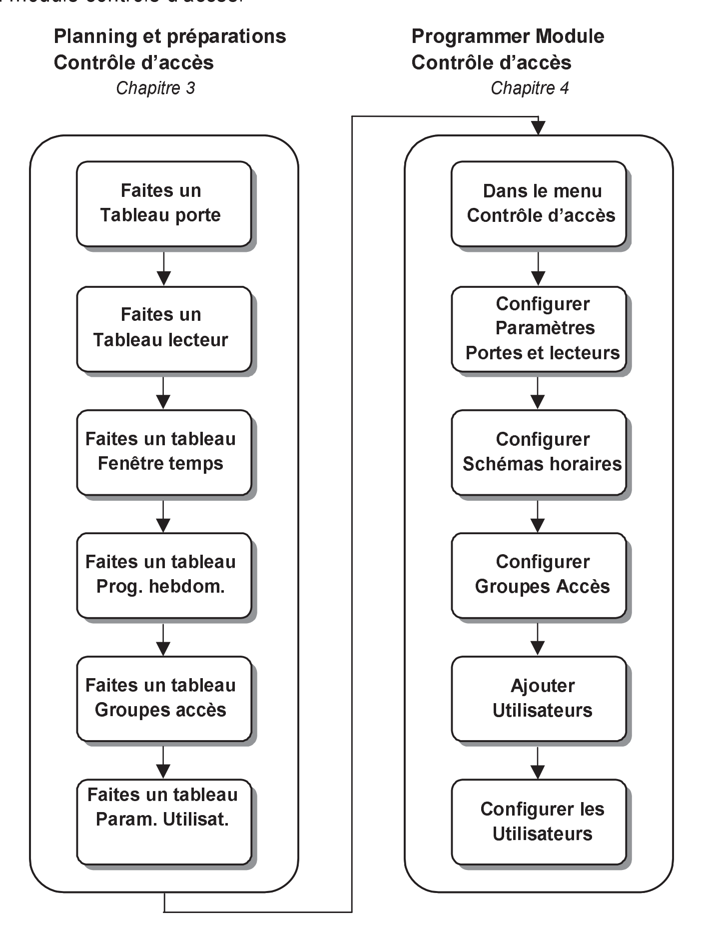


REMARQUE:
Les informations et exemples de ce manuel sont décrits dans le cas de l'utilisation du modèle ProSYS 128. Si vous avez installé le modèle ProSYS 16 ou le modèle ProSYS 40, tenez compte des limitations des caractéristiques du tableau ci-dessous.

Caractéristiques	ProSYS 16	ProSYS 40	ProSYS 128
Modules contrôle d'accès	2	4	8
Lecteurs	4	8	16
Partitions	4	4	8
Utilisateurs pour activer/désactiver	00-29	00-59	00-98
Utilisateurs Standards	100-349	100-999	100-999
Fenêtres de temps	15	25	25
Programme hebdomadaire	10	25	25
Groupes d'accès	8	16	16
Nombre d'entrées totales	8	16	32
Nombre de relais total	6	12	24

Processus du Contrôle d’accès

Le processus ci-dessous illustre la méthode conseillée pour le fonctionnement du module contrôle d’accès:



Chapitre 2: Utilisation du module contrôle d'accès

Le module contrôle d'accès peut être utilisé pour permettre l'accès entrée/sortie aux portes et pour l'armement/désarmement du système de sécurité.

Portes Entrée/Sortie

Les portes définies pour fonctionner en mode automatique sont accessibles en entrée/sortie par tous les utilisateurs qui possèdent des cartes ou des codes d'accès. La carte ou le code d'accès peut:

- ✦ Etre utilisé seulement pendant la fenêtre de temps assignée.
- ✦ Etre utilisé seulement aux portes attribuées.

De plus, des portes peuvent être programmées avec un état fixe (Toujours Ouvertes ou Toujours Fermées) ou être programmées pour qu'elles s'ouvrent quand un détecteur de mouvement observe un mouvement. Dans ce cas, les utilisateurs peuvent entrer/sortir normalement sans utiliser leur carte ou code d'accès.

➢ **Ouvrir une porte:**

- ✦ Présentez votre carte au lecteur ou utilisez votre code selon la méthode exigée (dépend du type de lecteur). Le système vérifie la carte ou le code (indication par une LED de confirmation et une tonalité bip) et ouvre ensuite la porte.



REMARQUES:

Si un faux code ou une carte invalide est introduit ou présenté cinq fois, un "Code Sabotage" est envoyé à la centrale ProSYS.

Les utilisateurs à Accès Seul ne peuvent pas accéder à une porte si le(s) partition(s) au(x)quelle(s) cette porte est attribuée est armée. (Consultez Attribuer utilisateurs Entrée/Sortie, page 19).

Armer/Désarmer le système

Le système peut seulement être armé/désarmé par les utilisateurs auxquels les droits d'armement/désarmement ont été attribués. Pour armer ou désarmer le système les critères suivants doivent être satisfaits:

- ✦ Le lecteur doit être autorisé pour les opérations d'armement/désarmement.
- ✦ Les cartes/codes d'accès doivent être programmés comme utilisateur armement/désarmement.
- ✦ Les cartes/codes d'accès peuvent seulement être utilisés durant la fenêtre de temps assignée.
- ✦ Les cartes/codes d'accès peuvent seulement être utilisés aux portes assignées.
- ✦ Les cartes/codes d'accès doivent être attribués aux partitions qui sont assignées à la porte et aux définitions de classification utilisateurs dans la centrale ProSYS .



REMARQUES:

Les utilisateurs peuvent effectuer un armement normal ou direct, selon le code d'armement. Demandez à votre installateur le code adéquat. Le système arme seulement les partitions qui sont d'application sur la porte, l'autorité utilisateur et les définitions d'armement utilisateur.

Armer le système

L'armement du système peut seulement être exécuté par les lecteurs qui disposent d'un clavier et qui sont autorisés pour l'armement.

➢ **Armer le système:**

- ✦ Si le lecteur est défini comme un type Clavier Seul, vous introduisez votre code d'armement suivi de votre code PIN:
  CODE ARMEMENT + [#] + CODE PIN + [#]
  -OU-
- ✦ Si le lecteur est défini comme un type Clavier + Carte (pour plus grande sécurité), introduisez votre code d'armement en utilisant le clavier, présentez votre carte d'accès au lecteur et ensuite introduisez votre code PIN:
  CODE ARMEMENT + [#] + PRESENTER CARTE + CODE PIN + [#]



IMPORTANT:
Si vous ne pouvez pas armer le système, consultez alors le *Supplément A, Pourquoi votre système ne s'arme pas*, page 25.

Désarmer le système

Le désarmement du système peut être effectué à partir de chaque lecteur qui est autorisé pour l'opération de désarmement.

➢ **Pour désarmer le système:**

- ✦ Si le lecteur est défini comme un type Clavier Seul, Carte Seul ou Clavier/Carte, introduisez votre code PIN en utilisant le clavier OU présentez votre carte d'accès au lecteur, selon ce qui est demandé:
  CODE PIN + [#] *OU* ***PRESENTER CARTE***
  -OU-
- ✦ Si le lecteur est défini comme un type Clavier + Carte, présentez votre carte d'accès au lecteur ET introduisez votre code PIN en utilisant le clavier:
  PRESENTER CARTE + CODE PIN + [#]

Désarmer sous contrainte

Vous pouvez également utiliser les lecteurs de contrôle d'accès (Clavier Seul, Clavier/Carte et Clavier + types de cartes) pour un désarmement sous contrainte. Ce type de désarmement envoie une alarme silencieuse au centre de surveillance tandis que vous désarmez le système sous contrainte.

Le "Code Contrainte" est automatiquement le numéro qui suit le code PIN de l'utilisateur (par ex : Code PIN = 1234; Code Contrainte = 1235). Consultez le *Manuel Utilisateur du ProSYS* pour plus de détails.

➢ **Désarmer sous contrainte :**

- ✦ Si le lecteur est défini comme un type Clavier Seul ou Clavier/Carte, introduisez la série de numéros suivante après votre code PIN:
  [CODE PIN + 1] + [#]
  -OU-
- ✦ Si le lecteur est défini comme un type Clavier + Carte, présentez votre carte d'accès au lecteur et ensuite introduisez la série de numéros suivante :
  PRESENTER CARTE + [CODE PIN + 1] + [#]

Chapitre 3: Planning et préparation du système contrôle d’accès

Avant de programmer le module contrôle d’accès, vous devez planifier comment le système fonctionne, durant quelles heures l’accès est permis via l’entrée principale, qui doit avoir accès aux zones spéciales du bâtiment, etc. Les éléments du planning recommandés pour la préparation des données qui seront utilisées durant la programmation sont décrits dans ce chapitre.

➢ **Planifier et préparer les données du contrôle d’accès:**

1) Etablissez un tableau qui contient pour chaque porte les données **porte** suivantes : numéro, nom, emplacement, mode et partition. Le tableau doit être basé sur les informations de votre installateur. (Consultez le tableau de la *Table 1: Portes*, page 27.)

2) Etablissez un tableau qui contient pour chaque lecteur les données **lecteur** suivantes : numéro, porte annexe, nom, type et possibilités d’armement/désarmement. Le tableau doit être basé sur les informations de votre installateur. (Consultez le tableau de le *Table 2: Lecteurs*, page 28).

3) Etablissez deux tableaux schéma horaire, comme décrit ci-dessous :

   Le but de ces schémas horaires est de donner à divers utilisateurs accès à des portes à des moments différents. Ceux-ci se composent de l’identification des différents types d’heures de travail ou autres divisions de temps dans les bâtiments et ensuite vous décidez quel schéma horaire sera utilisé.



REMARQUE:
Lorsque vous programmez les schémas horaires, vous devez d’abord programmer les fenêtres de temps et ensuite vous pouvez programmer les schémas hebdomadaires pour chaque groupe d’accès.

✦ Etablissez un tableau qui contient les données **fenêtre de temps** suivantes: numéro, nom schéma et un ou deux temps de début et de fin, selon ce qui est exigé. (Consultez le tableau de la *Table 3 : Fenêtres de Temps*, page 29.)

✦ Etablissez un tableau qui contient les données **programme hebdomadaire** suivantes: numéro, nom schéma et numéros de fenêtre de temps attribuées pour chaque jour de la semaine et pour les vacances. (Consultez le tableau de la *Table 4: Programmes hebdomadaires*, page 29).

4) Etablissez un tableau qui contient pour chaque groupe les données **groupe d'accès** suivantes : numéro, nom, portes permises et schéma hebdomadaire utilisé. Le but des groupes d'accès est d'identifier les différents départements ou zones dans la société et de décider quel groupe peut pénétrer dans quel département et à quel moment. (Consultez le tableau de la *Table 5: Groupes d'Accès*, page 31.)

5) Etablissez un tableau qui contient pour chaque utilisateur les données **utilisateur** suivantes : numéro, nom, numéro carte d'accès, code PIN et groupe d'accès attribué. Ce tableau vous permet de conservez facilement vos informations utilisateurs. (Consultez le tableau de la *Table 6: Paramètres Utilisateurs*, page 31.)

Chapitre 4: Programmer le module contrôle d'accès

Ce chapitre donne des instructions détaillées pour la programmation des fonctions du module contrôle d'accès, ainsi qu'une description des combinaisons touches rapides.



REMARQUE:
Les instructions de programmation décrites dans ce chapitre, sont basées sur les mêmes concepts que ceux décrits dans le manuel utilisateur ProSYS.

Ce chapitre comprend les paragraphes suivants :

Un nombre d'options de programmation pour le contrôle d'accès sont préprogrammées par l'installateur (consultez le *Manuel d'Installation et de Programmation du ProSYS*). De plus une description de la façon d'utiliser le clavier est présenté dans le *Manuel Utilisateur ProSYS.*



IMPORTANT:
Veillez à ce que votre système de sécurité soit désarmé avant de programmer une des fonctions du contrôle d'accès et aussi que tous les modules contrôle d'accès soient raccordés sur la centrale ProSYS.

Appelez le menu contrôle d’accès



Toutes les fonctions de ce manuel sont exécutées à partir du menu contrôle d’accès.

➢ **Appeler le menu contrôle d’accès :**

1) Appuyez sur la touche **[*]** pour ouvrir le menu utilisateur et sélectionnez ensuite **[8] Contrôle d’accès**.

   Le message suivant sera affiché :



2) Introduisez le code master ou le code manager et appuyez sur  .

   La première option du menu Contrôle d’accès est affichée, comme indiqué dans le paragraphe suivant. Vous pouvez maintenant programmer les options exigées, comme décrit dans les paragraphes suivants.

Configurer Portes et Lecteurs



La configuration des paramètres du contrôle d’accès implique la définition du mode porte pour chaque porte et du type de lecteur pour chaque lecteur du système:

- ✦ Définir mode porte, ci-dessous
- ✦ Définir type de lecteur (Reader type), page 11

Définir mode porte



Cette option vous permet de déterminer l’état de la serrure électrique sur chaque porte. Pendant le week-end vous voulez peut-être qu’une certaine porte soit tout le temps fermée pour éviter que des personnes n’entrent dans le bâtiment.

Si cette procédure est d’application, utilisez les données de la *Table 1 : Portes*, page 27.

➢ **Définir mode porte:**

1)


Sélectionnez le menu Contrôle d’accès **[1] Paramètres**.

2)
```
Paramètres:
1) Param. Porte
```

Sélectionnez **[1] Paramètre Porte**.

3)

```
Sélect une porte
01) Porte 01
```

Sélectionnez le numéro de porte adéquat et appuyez ensuite sur (Disarm) / (#/🔓).

4)

```
Porte 01 mode
1) Automatique
```

Définissez le mode porte (état de la serrure électrique de la porte) en sélectionnant le numéro d'option adéquat:

[1] Automatique: Défini le relais de porte en mode automatique. Ceci rend l'accès possible à un utilisateur ayant des droits d'accès lorsqu'il présente une carte ou un code au lecteur



REMARQUE:
C'est le mode porte standard qui est utilisé généralement pour des applications ordinaires

[2] Toujours Ouvert: Défini le relais de porte en mode toujours ouvert. Cette option garde la porte toujours ouverte et est utilisée quand vous voulez maintenir la porte ouverte mais sans générer d'alarme, par ex : le chargement et déchargement de marchandise.

[3] Toujours Fermé: Défini le relais de porte en mode toujours fermé. Cette option garde la porte toujours fermée et est utilisée pour éviter que des personnes utilisent la porte, par ex : durant le week-end.

Définir type de lecteur



L'option type de lecteur vous permet de définir le type d'accès et le niveau de sécurité pour chaque lecteur. Ceci implique de définir quel type de lecteur est installé sur chaque porte et de déterminer si le système peut être armé et/ou désarmé avec le lecteur. Vous pouvez par exemple avoir deux lecteurs à l'entrée de votre bâtiment mais vous voulez que le système soit seulement armé par le lecteur du côté intérieur et désarmé via le lecteur côté extérieur.



REMARQUES:
Le type de lecteur dépend du lecteur installé. Le système vous permet d'adapter différentes technologies lecteurs dans votre bâtiment, mais chaque module contrôle d'accès peut seulement accepter une technologie.

Si cette procédure est d'application, utilisez les données de la *Table 2: Lecteurs*, page 28.

➢ **Définir type de lecteur:**

1)

```
Contrôle d'accès:
1) Paramètres
```

Sélectionnez le menu Contrôle d'accès **[1] Paramètres**.

2)

```
Paramètres
1) Param. Porte
```

Sélectionnez **[2] Type Lecteur**

3)

```
Sélect un lecteur:
01) Lecteur 01
```

Sélectionnez le lecteur concerné et appuyez ensuite sur (Disarm) / (#/🔓).

4)

```
Type lect. carte
1) Carte Seul.
```

Définissez le type de lecteur (selon le type de lecteur installé) en sélectionnant l'option adéquate:

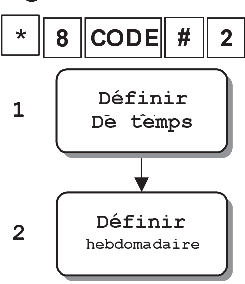
[1] Carte Seul.: Permet l'accès à une porte en utilisant une carte d'accès. Après avoir sélectionné cette option, choisissez **[O] Oui** ou **[N] Non** pour définir des droits de **désactivation**. (Cette option permet seulement aux utilisateurs de **désarmer** le système.)

[2] Code seul.: Permet l'accès à une porte en introduit un code au moyen du clavier installé. Après avoir sélectionné cette option, choisissez **[O] Oui** ou **[N] Non** pour définir des droits **d'activation** et ensuite lors de l'option suivante, choisissez **[O] Oui** ou **[N] Non** pour définir des droits de **désactivation**.

[3] Code ET Carte: Permet l'accès à une porte en utilisant une carte d'accès **ET** en introduisant un code au moyen du clavier installé. Après avoir sélectionné cette option, choisissez **[O] Oui** ou **[N] Non** pour définir des droits **d'activation** et ensuite lors de l'option suivante, choisissez **[O] Oui** ou **[N] Non** pour définir des droits de **désactivation**. (Cette option est utilisée pour une plus grande sécurité.)

[4] Code OU Carte: Permet l'accès à une porte **soit** en utilisant une carte d'accès **soit** en introduisant un code au moyen du clavier installé. Après avoir sélectionné cette option, choisissez **[O] Oui** ou **[N] Non** pour définir des droits de **désactivation**. (Cette option permet seulement aux utilisateurs de **désarmer** le système.)

Configurer les schémas horaires



Vous pouvez configurer les schémas horaires selon quels utilisateurs ont accès au système. Ceci implique de définir d'abord des fenêtres de temps journalières comme décrit ci-dessous, et ensuite de déterminer les programmes hebdomadaires basés sur les schémas des utilisateurs comme décrit page 14.



REMARQUE :
Les fenêtres de temps dans les programmes hebdomadaires qui sont définies pour les vacances fonctionnent pendant les dates des vacances qui sont définies dans l'option **[6][6][2]** du *Manuel Utilisateur du ProSYS* .

Définir des fenêtres de temps

L'option fenêtre de temps vous permet de créer des fenêtres de temps qui déterminent quand les utilisateurs ont accès au système. Vous pouvez définir au max. 25 fenêtres de temps qui se composent d'un nom logique et de deux intervalles de temps pour chaque fenêtre de temps. Vous devez définir des fenêtres de temps pour chaque groupe utilisateur. Ces fenêtres de temps seront utilisées plus tard pour constituer les programmes hebdomadaires de chaque groupe.

L'exemple suivant montre plusieurs fenêtres de temps qui sont définies pour permettre l'accès à différents groupes uniquement durant des périodes de temps déterminées:

Fenêtre de temps	Nom Fenêtre	Temps Début 1	Temps Stop 1	Temps Début 2	Temps Stop 2
1	Personnel de Marché	08:00	12:00	12:30	19:00
2	Jour de Nettoyage	08:00	12:00	12:30	16:00
3	Nuit de Nettoyage	15:00	19:00	19:30	23:00
4	Demi-jour de travail	08:00	14:00	14:00	14:00



REMARQUE:
Les intervalles de temps que vous définissez pour les fenêtres de temps doivent être en ordre **croissant** successif. Le système ne permet pas par exemple d'introduire un temps de début à **17:00** pour un temps de fin à **08:00** dans une fenêtre de temps spécifique.

Si cette procédure est d'application, utilisez les données de la *Table 3: Fenêtre de Temps*, page 29.

✦ **Définir une fenêtre de temps:**

1) `Contrôle d'accès:` / `1) Paramètres` — Sélectionnez à partir du menu Contrôle d'accès **[2] Schéma Horaire**

2) `Schéma horaire:` / `1) Fenêtre temps` — Sélectionnez **[1] Fenêtre de Temps**

3) `Sélect Fenêtre:` / `01) Fenêtre 01` — Introduisez un numéro de fenêtre de temps (1-25) et appuyez sur Disarm / #/🔓

4) `Fenêtre temps 01` / `DEBUT1: 00:00` — Introduisez l'heure du début du premier intervalle de temps en format HH:MM et appuyez sur Disarm / #/🔓

5) `Fenêtre temps 01` / `FIN1 : 00:00` — Introduisez l'heure de fin du premier intervalle de temps en format HH:MM et appuyez sur Disarm / #/🔓

6) `Fenêtre temps 01` / `DEBUT2: 00:00` — Introduisez l'heure du début du deuxième intervalle de temps et appuyez sur Disarm / #/🔓

7)

```
Fenêtre temps 01
FIN2 : 00:00
```

Introduisez l'heure de fin du deuxième intervalle de temps et appuyez sur Disarm / #

8)

```
Nom Fenêtre tps:
Fenêtre tps 01
```

Introduisez un nom logique pour la fenêtre de temps et appuyez sur Disarm / #

9)

```
Fenêtre temps 01
Est définie
```

Ce message indique que la fenêtre de temps a été définie avec succès.

Définir les programmes hebdomadaires



Cette option vous permet de définir les programmes hebdomadaires pour chaque groupe d'utilisateurs. Chaque programme hebdomadaire se compose de sept fenêtres de temps séparées et d'une fenêtre de temps vacances que vous sélectionnez, et qui détermine les jours et les intervalles de temps auxquels chaque groupe a accès au système.

La fenêtre de temps que vous sélectionnez pour la fenêtre temps vacances détermine comment sont définis les droits pour les groupes d'accès assignés lors d'une période de vacances.



REMARQUES:

Avant de définir les programmes hebdomadaires, vous devez d'abord définir les fenêtres de temps comme décrit au paragraphe précédent. Les programmes hebdomadaires sont nécessaires lorsque vous définissez des groupes d'accès comme décrit dans *Configurer des groupes d'accès*, page 16.

Vous pouvez définir jusque 25 programmes hebdomadaires. Vous pouvez par exemple composer un programme hebdomadaire ayant pour nom **Marché Hebdomadaire** et se composant de la fenêtre de temps **Personnel Marché** du lundi au jeudi; de la fenêtre de temps **Demis-jour de Travail** pour le vendredi; et la fenêtre de temps **Jamais** pour les week-ends et vacances, comme montré dans le tableau ci-après.

ID	Nom	Lu	Ma	Me	Je	Ve	Sa	Di	Vac
1	Marché Hebdomadaire	1	1	1	1	2	00	00	00
2	Nettoyage Nuit	3	3	3	3	2	00	00	00

- Fenêtre de temps 1: Personnel Marché
- Fenêtre de temps 2: Demi-jour de Travail
- Fenêtre de temps 00: Jamais

Si cette procédure est d’application, utilisez les données de la *Table 4: Programmes Hebdomadaire*, page 29

➢ **Définir un programme hebdomadaire:**

1)
```
Contrôle d’accès:
1) Paramètres
```
Sélectionnez à partir du menu Contrôle d’accès **[2] Schéma horaire**

2)
```
Schéma horaire:
1) Fenêtre temps
```
Sélectionnez [2] **Programme hebdomadaire**

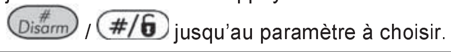
3)
```
Sélect. fenêtre:
01) Semaine 01
```
Introduisez un numéro de programme hebdomadaire (1-25) et appuyez sur



4)
```
Sélect jour:
1) Dimanche
```
Sélectionnez **[1] Dimanche** et appuyez sur



5)
```
Prog Schéma hor.
01) Toujours
```
Attribuez une fenêtre de temps pour dimanche et faisant défiler la liste des fenêtres de temps journalières définies et appuyez ensuite sur



jusqu’au paramètre à choisir.



REMARQUE:
En plus de la liste des fenêtres de temps définies dans le système, les options **[00] Toujours** (standard) et **[01] Jamais** sont disponibles.

6)
```
Sélect jour
2) Lundi
```
L’option pour le jour suivant est automatiquement affichée.



REMARQUE:
Vous pouvez appuyer sur [∗] à tout moment durant la programmation pour quitter l’option programme hebdomadaire et enregistrer les modifications définies.

7) Répétez les étapes de 4 à 6 pour les autres jours de la semaine (ainsi que pour l’option **[8] Vacances**)

8)
```
Nom fenêtre temps
Hebdom. 01
```
Introduisez un nom logique pour un programme hebdomadaire. Par exemple, **Marché Hebdomadaire** (max. 12 caractères) et appuyez sur **Enter**.

Configurer des groupes d'accès

| * | 8 | CODE | # | 3 |

Après avoir défini le mode porte, le type lecteur, les schémas horaires, vous pouvez configurer les groupes d'accès. Chaque groupe d'accès représente les portes auxquelles les groupes d'utilisateurs ont accès durant des périodes spécifiques.

Vous pouvez configurer jusque 16 groupes d'accès, ce qui consiste en l'attribution d'un nom logique à un groupe d'accès et en l'attribution de max. 16 portes, chacune avec son propre programme hebdomadaire selon le groupe d'accès concerné. Après cela, vous pouvez assigner chaque utilisateur au groupe d'accès adéquat, comme décrit dans *Attribuer utilisateurs aux groupes d'accès*, page 24.

Vous pouvez par exemple configurer un groupe d'accès avec le nom **Personnel de Marché**, qui représente un groupe d'utilisateurs ayant accès aux portes 1, 7 et 8, conformément au programme hebdomadaire ayant pour nom **Marché hebdomadaire** défini plus tôt. Ensuite vous pouvez définir un autre groupe d'accès ayant pour nom **Personnel de nettoyage**, qui représente un groupe d'utilisateurs pouvant accéder aux portes 7 et 8 et seulement durant les périodes horaires définies dans le programme hebdomadaire **Nettoyage Nuit** (par ex: Lu-Ve, 17:00 à 19:00).



REMARQUE:
Les modifications que vous apportez dans les définitions des groupes d'accès, influencent directement les utilisateurs qui sont attribués à ces groupes

Si cette procédure est d'application, utilisez les données de la *Table 5: Groupes d'accès*, page 31.

✦ **Configurer un groupe d'accès:**

1) `Contrôle d'accès:` `1) Paramètres` — Sélectionnez à partir du menu Contrôle d'accès **[3] Groupe accès**.

2) `Sélect. groupe:` `01) Groupe 01` — Introduisez un numéro de groupe (1-16).

3) `Sélect. Porte` `1) Porte 01` — Sélectionnez un numéro de porte pour le groupe sélectionné et appuyez sur Disarm / #/🔓.

4) `Progr. Hebd D=01` `00) Toujours` — Sélectionnez un programme hebdomadaire (1-25) pour la porte sélectionnée et appuyez Disarm / #/🔓.



REMARQUE:
En plus de la liste des programmes hebdomadaires définis dans le système, les options **[00] Toujours** (standard) et **[01] Jamais** sont disponibles.

5) Répétez les étapes 3 et 4 pour définir les portes restantes et leurs programmes hebdomadaires pour le groupe d'accès, si nécessaire.

6)

```
Donnez Nom Grp
Groupe 01
```

Après avoir sélectionné les programmes hebdomadaires pour les portes disponibles, cette option s'affiche. Introduisez un nom logique pour le groupe et appuyez sur / .

7)

```
Groupe d'accès 01
Est défini
```

Ce message indique que le groupe d'accès a été défini avec succès.

Ajouter des cartes et des utilisateurs au système



L'option "Lire Cartes" vous permet d'ajouter deux types d'utilisateurs au système:

- ✦ **Ajouter Utilisateurs Armer/Désarmer**, page 17
- ✦ **Ajouter Utilisateurs Standard**, page 19



REMARQUE:
Cette option est uniquement activée quand le module contrôle d'accès est sur le système de sécurité.

Si cette procédure est d'application, utilisez les données de la *Table 6: Paramètres Utilisateurs*, page 31.

Quand une introduction échoue ! Lorsque deux types sont ajoutés au système, si le numéro utilisateur est déjà utilisé, un message apparaît vous donnant l'option d'écraser la donné utilisateur. De plus un message est apparaît suivi de trois bips, si le code de la carte est déjà utilisé dans le système pour indiquer que le code de la carte existe déjà.

Ajouter des Utilisateurs Armer/Désarmer



Cette option vous permet d'ajouter le nombre de carte maximum défini dans votre système de sécurité avec les droits d'accès armer/désarmer:

- ✦ **En introduisant un code carte**, décrit ci-dessous
- ✦ **En présentant une carte à un lecteur**, page 19

Lorsque des utilisateurs pouvant armer/désarmer sont ajoutés, vous devez aussi sélectionner les partitions qui peuvent être armées/désarmées par chaque utilisateur. Vous pouvez par exemple attribuer seulement les partitions 1, 2 et 3 pour permettre à l'utilisateur d'armer/désarmer le département marketing et les cuisines, mais d'interdire l'armement/désarmement d'autres zones qui font parties des bureaux de management (pour cela un "trajet" est créé).



REMARQUES:

Les utilisateurs ne peuvent armer/désarmer dans le système que pour les lecteurs pour lesquels vous avez configuré des possibilités d'armement/désarmement dans les définitions du type de lecteurs (Voir *Définir type de lecteur*, page 11).

Le système arme seulement les partitions qui sont d'application sur la porte, et selon les droits de l'utilisateur et les définitions utilisateur pour l'armement.

Ajouter en introduisant un code carte



Vous pouvez ajouter des utilisateurs pour armer/désarmer le système en introduisant le code de 8 chiffres qui est imprimé sur la carte d'accès via un clavier installé. Ceci vous permet d'ajouter des utilisateurs à l'aide de la programmation à distance.

Cette option est recommandée lorsque des cartes RISCO Group sont utilisées. Celles-ci possèdent sur le côté supérieur un numéro de 8 chiffres. Si vous utilisez d'autres cartes que celles de RISCO Group ou des cartes avec moins de 8 chiffres, il est conseillé d'ajouter des utilisateurs en présentant les cartes, comme décrit dans "*Ajouter en présentant une carte au lecteur*", page 19.

✦ **Ajouter un utilisateur pour armer/désarmer en introduisant un code carte:**

1)
```
Contrôle d'accès:
1) Paramètres
```
Sélectionnez à partir du menu Contrôle d'accès **[4] Lire Cartes**

2)
```
Progr. Cartes
1) Cartes 'ON'
```
Sélectionnez **[1] Cartes 'ON'**

3)
```
Cartes ON  00-98
1)Avec code carte
```
Sélectionnez **[1] Avec code carte**

4)
```
Sélect Utilisat.:
00        (00-98)
```
Introduisez un numéro utilisateur entre 00-98 et appuyez sur Disarm / #/🔓. Le premier numéro utilisateur disponible est donné comme base.

5)
```
P=12345678  U=00
  O.......
```
Attribuez de 1 à 8 partitions à l'utilisateur en plaçant avec la touche Stay / 🔒 **[O] Oui** ou **[N] Non** sous les numéros de partitions souhaités et appuyez ensuite sur Disarm / #/🔓.

6)
```
U:00 Code Carte
--------
```
Introduisez le code carte de 8 chiffres de la carte d'accès que vous voulez à l'utilisateur et appuyez sur Disarm / #/🔓.

7)
```
U:00 Introductio
  confirmée
```
Ce message indique que l'utilisateur pour armer/désarmer a été ajouté au système avec succès.

Ajouter en présentant une carte à un lecteur

*	8	CODE	#	4	1	2

Vous pouvez ajouter des utilisateurs pour armer/désarmer le système en présentant au lecteur la carte de chaque utilisateur. Cette option est recommandée si vous avez des cartes d'accès sans numéros imprimés sur la carte ou lorsque les cartes possèdent moins de 8 chiffres imprimés.

✦ **Ajouter un utilisateur armer/désarmer en présentant une carte à un lecteur:**

1)
```
Contrôle d'accès:
1) Paramètres
```
Sélectionnez à partir du menu Contrôle d'accès **[4] Lire Cartes**

2)
```
Progr. Cartes
1) Cartes 'ON'
```
Sélectionnez **[1] Cartes 'ON'**

3)
```
Carte ON    00-98
1)Avec code carte
```
Sélectionnez **[2] Via lecteur**. La LED verte du lecteur clignote pendant 12 secondes tandis le lecteur attend la carte. Si vous ne présentez pas de carte, le lecteur donne un bip de défaut.

4)
```
Définition empl.
Lecteur: 01
```
Sélectionnez le numéro du lecteur que vous voulez utiliser pour l'introduction et appuyez sur 

.

5)
```
Sélect. Utilisat:
00        (00-98)
```
Introduisez un numéro utilisateur entre 00-98 et appuyez sur Disarm / #/.

6)
```
P=12345678  U=00
  O.......
```
Attribuez de 1 à 8 partitions à l'utilisateur en plaçant avec la touche Stay / **[O] Oui** ou **[N] Non** sous les numéros de partitions souhaités et appuyez ensuite sur Disarm / #/.

7)
```
Présenter votre
Carte au lecteur
```
Présentez la carte au lecteur et attendez et attendez le bip de confirmation.

8)
```
U:00 Introduction
acceptée
```
Ce message indique que l'utilisateur pour armer/désarmer a été ajouté au système avec succès.

Ajouter des Utilisateurs Standards



Vous pouvez ajouter jusque 999 utilisateurs ayant des droits d'accès de base et cela des façons suivantes:

- ✦ **En introduisant un groupe de codes cartes**, décrit ci-dessous
- ✦ **En introduisant des codes cartes un par un**, page 21
- ✦ **En présentant une carte au lecteur**, page 22



REMARQUE:
Les utilisateurs standard peuvent seulement ouvrir des portes; ils ne peuvent ni armer ni désarmer le système.

Si vous avez plusieurs catégories d'utilisateurs, il est recommandé d'attribuer un bloc de numéros séparés à chaque groupe d'accès. Cela sera plus facile pour diviser chaque catégorie lors de schéma horaire. Vous pouvez par exemple attribuer les numéros utilisateurs de 100 à 199 au groupe d'accès 1, 200 à 299 au groupe d'accès 2, etc.

Ajouter en introduisant un groupe de codes cartes

| * | 8 | CODE | # | 4 | 2 | 1 | 1 |

Vous pouvez ajouter un groupe d'utilisateurs standard en attribuant une pile de cartes par ordre croissant successif. Vous pouvez par exemple ajouter un groupe de 100 cartes avec des numéros successifs en introduisant seulement le premier code carte, après quoi le système introduit automatiquement le reste de l'information.



REMARQUE:
Si pendant l'introduction des codes cartes pour un groupe dans le système un problème est observé, le processus est automatiquement arrêté.

✦ **Introduire des codes cartes pour un groupe d'utilisateurs entrée/sortie:**

1) `Contrôle d'accès:` / `1) Paramètres` — Sélectionnez à partir du menu Contrôle d'accès **[4] Lire Cartes**

2) `Progr. Cartes` / `1) Cartes 'ON'` — Sélectionnez **[2] Carte d'accès**

3) `Carte acc. 100-999` / `1)Avec code carte` — Sélectionnez **[1] Avec code carte**

4) `Attribution Code` / `1) Par Groupe` — Sélectionnez **[1] Par groupe**

5) `Premier N° Util.` / `100    100-999` — Introduisez un numéro utilisateur entre 100-999 et appuyez sur [Disarm #] / [#/🔓]. Le premier numéro utilisateur disponible est donné comme base.

6) `Nombre Util.` / `Du Groupe:001` — Introduisez le nombre d'utilisateurs appartenant au groupe que vous voulez ajouter au système et appuyez sur [Disarm #] / [#/🔓].

7)
```
Prem. code carte
--------
```
Introduisez le numéro à 8 chiffres du code de la carte d'accès que vous voulez attribuer au premier utilisateur dans le groupe et appuyez Disarm / #/. Le système attribue automatiquement un numéro de code carte successif à chaque utilisateur dans le groupe.

8)
```
Introd. Groupe
acceptée
```
Ce message indique que le groupe d'utilisateurs standard a été ajouté au système avec succès

Ajouter en introduisant des codes cartes un par un



Vous pouvez ajouter un groupe d'utilisateurs standard un par un. Cette option est utilisée quand un nombre de cartes dont les numéros ne se suivent pas doit être attribuées ou quand vous devez attribuer un nombre de cartes à l'aide d'un clavier qui n'est pas placé près d'un lecteur.

Si le code de la carte d'accès contient moins de 8 caractères, il est conseillé de présenter la carte au lecteur au lieu d'introduire des zéros pour les chiffres restants. Voir *Ajouter en présentant une carte au lecteur*, page 22.

✦ **Introduire un par un les codes cartes pour un groupe d'utilisateurs entrée/sortie:**

1)
```
Contrôle d'accès:
1) Paramètres
```
Sélectionnez à partir du menu Contrôle d'accès **[4] Lire Cartes**

2)
```
Progr. Cartes
1) Cartes 'ON'
```
Sélectionnez **[2] Carte d'accès**

3)
```
Carte acc. 100-999
1) Avec code carte
```
Sélectionnez **[1] Avec code carte**

4)
```
Attribution Code
1) Par Groupe
```
Sélectionnez **[2] Un par Un**

5)
```
Sélect. Util.:
100    100-999
```
Introduisez un numéro utilisateur entre 100-999 et appuyez sur Disarm / #/. Le premier numéro utilisateur disponible est donné comme base.

6)
```
U:100 Code carte
--------
```
Introduisez le code à 8 chiffres de la carte d'accès que vous voulez attribuer au premier utilisateur et appuyez Disarm / #/.

7)
```
U: 100 Introd.
acceptée
```
Ce message indique que le premier utilisateur standard a été ajouté avec succès au système. Ensuite l'option **Sélect. Util.** est à nouveau affichée.

8) Répétez les étapes de 5 à 7 pour ajouter les autres utilisateurs de groupe.

Ajouter en présentant une carte au lecteur

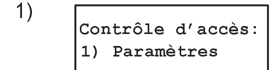
*	8	CODE	#	4	2	2

Vous pouvez ajouter des utilisateurs standard en présentant la carte de chaque utilisateur au lecteur.

Cette option est utilisée dans les circonstances suivantes:

- ✦ Quand vous avez des cartes d'accès sans numéro.
- ✦ Quand les cartes comportent moins de huit chiffres.
- ✦ Quand vous avez une pile de cartes dont les numéros ne se suivent pas.

✦ Ajouter un utilisateur standard en présentant une carte au lecteur:

1) 

Sélectionnez à partir du menu Contrôle d'accès **[4] Lire Cartes**

2)
```
Progr. Cartes
1) Cartes 'ON'
```

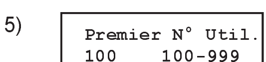
Sélectionnez **[2] Carte d'accès**

3)
```
Carte acc. 100-999
1) Avec code carte
```

Sélectionnez **[2] Via lecture**

4)
```
Définition empl.
Lecteur: 01
```

Sélectionnez le numéro du lecteur que vous voulez utiliser pour l'introduction et appuyez sur Disarm / #/.

5) 

Introduisez un numéro utilisateur entre 100-999 et appuyez sur Disarm / #/. Le premier numéro utilisateur disponible est donné comme base.

6)
```
Présenter votre
Carte au lecteur
```

Présentez la carte au lecteur et attendez et attendez le bip de confirmation.

7)
```
U:00 Introductio
acceptée
```

Ce message indique que l'utilisateur standard a été ajouté avec succès au système.



REMARQUE:
Si vous effectuez cette procédure sur un lecteur qui est éloigné du clavier, vous ne verrez pas le message ci-dessus car il s'affiche seulement pendant quelques secondes.

8) Répétez l'étape 6 pour introduire les autres cartes.

9) Pour arrêter la procédure d'enregistrement, présentez une carte qui a déjà été introduite.

Configurer les paramètres utilisateurs



Vous pouvez définir des paramètres pour les utilisateurs du système, comprenant l'attribution des codes PIN (codes utilisateurs), l'attribution des utilisateurs à des groupes d'accès spécifiques et l'effacement des utilisateurs, comme décrit dans les paragraphes suivants:

- ✦ **Attribuer des codes PIN**, page 23
- ✦ **Attribuer les utilisateurs aux groupes d'accès**, page 24
- ✦ **Effacer des utilisateurs**, page 24

Attribuer des codes PIN



L'option code PIN vous permet d'attribuer un code PIN à chaque utilisateur, ce code est nécessaire lorsque votre système comprend des lecteurs avec clavier intégré. Le système attribue automatiquement un code "Sous contrainte" (code PIN augmenté de 1)

Par exemple : code PIN = 1234; code "Sous contrainte" = 1235. C'est pourquoi, vous ne pouvez pas attribuer aux utilisateurs du système des codes PIN successifs. Vous pouvez utiliser un numéro sur deux, par exemple : 1234, 1236, 1238, etc.



REMARQUES:
Le **CODE PIN** doit être défini après l'attribution d'une carte à un utilisateur, autrement celle-ci sera effacée.
Pour les utilisateurs **00-98,** il est conseillé d'utiliser le même code PIN que celui utilisé dans votre système de sécurité.
Si par malchance un numéro successif est utilisé, le message suivant s'affiche: **Code non accepté**

✦ **Attribuer un code PIN:**

1)	Contrôle d'accès: 1) Paramètres	Sélectionnez à partir du menu Contrôle d'accès **[5] Paramètre Utilisateur**
2)	Paramètre Util. 1) Code Util.	Sélectionnez **[1] Code Utilisateur**
3)	Introd. Util.: 000	Introduisez le numéro utilisateur et appuyez sur # Disarm / #/🔓.
4)	Introd Code Util:	Introduisez le code PIN de l'utilisateur et appuyez sur # Disarm / #/🔓.
5)	Code Accepté	Ce message indique que le code PIN a été attribué au système avec succès

Attribuer des utilisateurs aux groupes d'accès

*	8	CODE	#	5	2

Vous pouvez attribuer un utilisateur ou des groupes d'utilisateurs au groupe d'accès concernés, cela est effectué en définissant une série d'utilisateurs et ensuite en attribuant cette série au groupe d'accès. Chaque utilisateur que vous attribuez à un groupe aura accès au système, selon les paramètres sélectionnés pendant la configuration du groupe d'accès concerné (consultez *Configurer des groupes d'accès*, page 16).



REMARQUE:
Chaque utilisateur du système ne peut être attribué uniquement qu'à un seul groupe d'accès.

✦ **Attribuer des utilisateurs à des groupes d'accès:**

1)
```
Contrôle d'accès:
1) Paramètres
```
Sélectionnez à partir du menu Contrôle d'accès **[5] Paramètre Utilisateur**

2)
```
Paramètre Util.
1) Code Util.
```
Sélectionnez **[2] Attribuer Groupe**

3)
```
Introd. Util.:
DE 000 A 000
```
Introduisez le premier et le dernier numéro utilisateur de la série d'utilisateurs que vous souhaitez ajouter au groupe d'accès et





REMARQUE:
Quand une série d'utilisateur est introduite, le numéro introduit dans le champ DE doit toujours être inférieur ou identique à celui introduit dans le champ A.

4)
```
Attribuer Groupe:
01) Groupe 01
```
Introduisez un numéro de groupe (01-16) et appuyez sur Disarm / #/6.

5)
```
Attribution Groupe
confirmée
```
Le message suivant s'affiche pour confirmer que l'attribution groupe a été réussie.

Effacer les utilisateurs



L'option Effacer Utilisateur vous permet d'effacer du système un ou des groupes d'utilisateurs. C'est par exemple nécessaire quand un utilisateur perd sa carte ou quand un utilisateur particulier ne travaille plus dans la société et donc ne peut plus avoir accès au bâtiment.

✦ **Effacer un utilisateur du système:**

1)
```
Contrôle d'accès:
1) Paramètres
```
Sélectionnez à partir du menu Contrôle d'accès **[5] Paramètre Utilisateur**

2)
```
Paramètre Util.
1) Code Util.
```
Sélectionnez **[3] Effacer Code**

3)
```
Introd. Util.:
DE 000 A 000
```
Introduisez le premier et le dernier numéro utilisateur de la série d'utilisateurs que vous souhaitez effacer et appuyez sur





REMARQUE:
Quand une série d'utilisateur est introduite, le numéro introduit dans le champ **DE** doit toujours être inférieur ou identique à celui introduit dans le champ **A**.

4)
```
***Effacer***
Etes vous sur?  N
```
Sélectionnez avec la touche Stay / **[O] Oui** ou **[N] Non** et appuyez ensuite sur Disarm / #.

5)
```
Util. effacé
```
Ce message indique que l'utilisateur a été effacé avec succès.

Ouvrir portes



Vous pouvez utiliser le système de sécurité pour ouvrir une porte à distance à l'aide d'un clavier qui a été prédéfini dans le système.



REMARQUE:
Seul les niveaux d'autorité Responsable Général ou Manageur peuvent exécuter cette procédure.

✦ **Ouvrir une porte:**

1)
```
Contrôle d'accès:
1) Paramètres
```
Sélectionnez à partir du menu Contrôle d'accès **[6] Ouvrir porte**

2)
```
Sélect une porte:
01) Porte 01
```
Sélectionnez le numéro de la porte concernée et appuyez ensuite sur Disarm / #.

3)
```
Porte 01 est
ouverte
```
La porte sélectionnée est ouverte et ce message de confirmation est affichée.

Supplément A: Pourquoi votre système ne s’arme t’il pas?

Quand vous ne réussissez pas à armer le système, contrôlez alors si les critères suivants sont bien remplis:

- Les partitions que vous désirez armer sont prêtes pour l’armement.



PENSEZ-Y:
Seul sont activées les partitions auxquelles l’utilisateur accès est attribué, la partition incluant la porte.

- L’utilisateur est défini comme un utilisateur pour Armer/Désarmer.
- L’utilisateur est attribué au bon groupe d’accès.



PENSEZ-Y:
Avant de définir un groupe d’accès, vous devez d’abord définir un programme hebdomadaire et l’attribuer à une porte.

- L’utilisation de carte/code s’effectue dans la fenêtre de temps autorisée.
- Le code d’armement correct est introduit. (Demandez à votre installateur le code d’usine, si nécessaire.)
- Le code PIN correct est introduit.
- Le lecteur est autorisé pour l’opération d’armement.

Supplément B: Tables de Planning et de Préparations

Table 1: Portes

Porte n°	Porte	Emplacement Porte	Mode porte	Paramètre porte
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Modes Porte: Automatique, Toujours Ouvert et Toujours Fermé

Table 2: Lecteurs

Lecteur n°	Associer à la porte	Nom Lecteur	Type Lecteur	Armer O/N	Désarmer O/N
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

Type Lecteur: [1] Carte Seul; [2] Clavier Seul; [3] Carte + Clavier; [4] Carte/Clavier

Table 3: Fenêtres de Temps

N°	Nom Programme	Début 1 HH:MM	Fin 1 HH:MM	Début 2 HH:MM	Fin 2 HH:MM

REMARQUE:
Les intervalles de temps que vous définissez pour les fenêtres de temps doivent être **augmentés** successivement. Le système ne permet pas par exemple d'introduire un temps de début à **17:00** pour un temps de fin à **08:00** dans une fenêtre de temps spécifique.

Table 4: Programmes Hebdomadaires

		Attribution Fenêtre de Temps							
Non	Nom Programme	Di	Lu	Ma	Me	Je	Ve	Sa	Vac.

Table 5: Groupes d’accès

N°	Nom Groupe	Portes d’accès	Programme hebdomadaire
1	Marketing		



REMARQUE:
Le tableau ci-dessus explique comment vous pouvez définir une information pour chaque groupe d’accès avec maximum 16 portes d’accès. Copiez ce tableau si nécessaire en cas de groupes d’accès supplémentaires dans votre système.

Table 6: Paramètres Utilisateurs

Utilisateurs n°	Nom Utilisateur	Code carte #	PIN #	Groupe d’accès

Recommandations personnelles

Recommandations personnelles

RISCO Group GARANTIE LIMITEE

RISCO Group ses sous-traitants et filiales ("Vendeur") garantissent que leurs produits sont sans défaut en ce qui concerne le matériel et la finition pour un usage normal pendant 24 mois à partir de la date de production. Parce que le vendeur n’installe, ni ne raccorde lui-même le produit et parce que le produit peut être utilisé en liaison avec des produits qui ne sont pas fabriqués par le vendeur, le vendeur ne peut pas garantir le fonctionnement du système de protection qui utilise ce produit. L’obligation et la responsabilité du vendeur sur le plan de cette garantie sont expressément limitées aux réparations et aux remplacements, selon le choix du Vendeur, endéans un temps raisonnable selon la date de livraison, d’un seul produit qui ne satisfait pas aux spécifications. Le vendeur n’offre aucune autre garantie, explicite ou implicite, et ne donne pas de garantie en vue de débit facile ou d’opportunité pour un but spécifique.

Dans aucun cas le vendeur ne sera responsable pour d’éventuels dommages accidentels, pour tentative de violation de cette garantie, explicite ou implicite, ou en raison d’autre base de responsabilité.

L’obligation du vendeur sur le plan de cette garantie ne comprendra pas de frais de transport ou de frais installation ou de responsabilité directe et indirecte ou de dommage ou retard.

Le vendeur ne déclare pas que son produit ne peut pas être mis en erreur ou doublé, que le produit prévient les dommages personnels ou perte de biens par vol, pillage, incendie ou autre; ou que le produit dans chaque cas offrira un avertissement ou protection adéquate. C’est l’acheteur qui peut diminuer le risque de vol, pillage ou incendie sans avertissement par une alarme correctement installée et entretenue, mais il n’y a aucune assurance ou garantie que cela ne surviendra pas ni qu’aucun dommage personnel ou perte de biens n’en résultera.

Comme conséquence de cela, le vendeur ne porte aucune personnalité dans le cas d’éventuels dommages personnels, dégâts aux biens ou perte de ceux-ci, venant d’une réclamation signifiant que le produit n’a pas donné d’avertissement. Si cependant le vendeur a une responsabilité, une garantie limitée sera appliquée pour perte ou dommage direct ou indirect, malgré la cause ou l’origine, la responsabilité maximale du vendeur ne sera pas plus élevée que le prix de vente du produit, qui sera le seul moyen de recours contre le vendeur.

Aucun collaborateur ou représentant du vendeur n’est autorisé à modifier cette garantie de quelque manière que ce soit ni à offrir une autre garantie.

AVERTISSEMENT: Ce produit doit au moins être testé une fois par semaine.

Contactez RISCO Group

RISCO Group offre un service clientèle et un support produit. Vous pouvez nous contacter via notre website (www.riscogroup.com)
ou via les numéros de téléphone et de fax suivants:

Royaume Uni
Tel: +44-161-655-5500
technical@riscogroup.co.uk

Italie
Tel: +39-02-66590054
support@riscogroup.it

Espagne
Tel: +34-91-490-2133
support-es@riscogroup.com

France
Tel: +33-164-73-28-50
support-fr@riscogroup.com

Belgique
Tel: +32-2522-7622
support-be@riscogroup.com

États-Unis
Tel: +305-592-3820
support@riscogroupusa.com

Brésil
Tel: +55-11-3661-8767
support-br@riscogroup.com

Chine
Tel: +86-21-52-39-0066
support-cn@riscogroup.com

Poland
Tel: +48-22-500-28-40
support-pl@riscogroup.com

Israël
Tel: +972-3-963-7777
support@riscogroup.com



5IN128EACUMFR B